

## **COMMITTEE AMENDMENT**

[STAFF WORKING DRAFT]

May 14, 2002

Purpose: To make changes in the bill as introduced.

**IN THE COMMITTEE ON COMMERCE, SCIENCE, AND  
TRANSPORTATION** —107TH Cong., 2D Sess.

**S. 2182**, 107TH Congress, 2D Session

MAY 16, 2002

INTENDED to be proposed by Mr. WYDEN (for himself and  
Mr. EDWARDS)

Viz: Strike out all after the enacting clause and insert the  
following:

1 **SECTION 1. SHORT TITLE.**

2       This Act may be cited as the “Cyber Security Re-  
3 search and Development Act”.

4 **SEC. 2. FINDINGS.**

5       The Congress finds the following:

6           (1) Revolutionary advancements in computing  
7       and communications technology have interconnected  
8       government, commercial, scientific, and educational  
9       infrastructures—including critical infrastructures for  
10      electric power, natural gas and petroleum production  
11      and distribution, telecommunications, transportation,  
12      water supply, banking and finance, and emergency

1       and government services—in a vast, interdependent  
2       physical and electronic network.

3           (2) Exponential increases in interconnectivity  
4       have facilitated enhanced communications, economic  
5       growth, and the delivery of services critical to the  
6       public welfare, but have also increased the con-  
7       sequences of temporary or prolonged failure.

8           (3) A Department of Defense Joint Task Force  
9       concluded after a 1997 United States information  
10      warfare exercise that the results “clearly dem-  
11      onstrated our lack of preparation for a coordinated  
12      cyber and physical attack on our critical military  
13      and civilian infrastructure”.

14          (4) Computer security technology and systems  
15      implementation lack—

16           (A) sufficient long term research funding;

17           (B) adequate coordination across Federal  
18      and State government agencies and among gov-  
19      ernment, academia, and industry; and

20           (C) sufficient numbers of outstanding re-  
21      searchers in the field.

22          (5) Accordingly, Federal investment in com-  
23      puter and network security research and develop-  
24      ment must be significantly increased to—

1 (A) improve vulnerability assessment and  
2 technological and systems solutions;

3 (B) expand and improve the pool of infor-  
4 mation security professionals, including re-  
5 searchers, in the United States workforce; and

6 (C) better coordinate information sharing  
7 and collaboration among industry, government,  
8 and academic research projects.

9 (6) While African-Americans, Hispanics, and  
10 Native Americans constitute 25 percent of the total  
11 United States workforce and 30 percent of the col-  
12 lege-age population, members of these minorities  
13 comprise less than 7 percent of the United States  
14 computer and information science workforce.

15 **SEC. 3. DEFINITIONS.**

16 For purposes of this Act—

17 (1) the term “Director” means the Director of  
18 the National Science Foundation;

19 (2) the term “institution of higher education”  
20 has the meaning given that term in section 101 of  
21 the Higher Education Act of 1965 (20 U.S.C.  
22 1001); and

23 (3) “Federal agency benchmark security stand-  
24 ards” means a baseline minimum security configura-  
25 tion for specific computer hardware or software com-

1       ponents, an operational procedure or practice, or or-  
2       ganizational structure that increases the security of  
3       the information technology assets of a department or  
4       agency of the Federal Government.

5   **SEC. 4. NATIONAL SCIENCE FOUNDATION RESEARCH.**

6       (a) COMPUTER AND NETWORK SECURITY RESEARCH  
7   GRANTS.—

8           (1) IN GENERAL.—The Director shall award  
9       grants for basic research on innovative approaches  
10      to the structure of computer and network hardware  
11      and software that are aimed at enhancing computer  
12      security. Research areas may include—

13                   (A) authentication and cryptography;

14                   (B) computer forensics and intrusion de-  
15      tection;

16                   (C) reliability of computer and network ap-  
17      plications, middleware, operating systems, and  
18      communications infrastructure;

19                   (D) privacy and confidentiality;

20                   (E) network security architecture, includ-  
21      ing tools for security administration and anal-  
22      ysis such as firewall technology;

23                   (F) emerging threats, including malicious  
24      such as viruses and worms;

1 (G) vulnerability assessments and tech-  
2 niques for quantifying risk;

3 (H) operations and control systems man-  
4 agement;

5 (I) management of interoperable digital  
6 certificates or digital watermarking; and

7 (J) remote access and wireless security.

8 (2) MERIT REVIEW; COMPETITION.—Grants  
9 shall be awarded under this section on a merit-re-  
10 viewed competitive basis.

11 (3) AUTHORIZATION OF APPROPRIATIONS.—  
12 There are authorized to be appropriated to the Na-  
13 tional Science Foundation to carry out this  
14 subsection—

15 (A) \$35,000,000 for fiscal year 2003;

16 (B) \$40,000,000 for fiscal year 2004;

17 (C) \$46,000,000 for fiscal year 2005;

18 (D) \$52,000,000 for fiscal year 2006; and

19 (E) \$60,000,000 for fiscal year 2007.

20 (b) COMPUTER AND NETWORK SECURITY RESEARCH  
21 CENTERS.—

22 (1) IN GENERAL.—The Director shall award  
23 multiyear grants, subject to the availability of appro-  
24 priations, to institutions of higher education (or con-  
25 sortia thereof) to establish multidisciplinary Centers

1       for Computer and Network Security Research. Insti-  
2       tutions of higher education (or consortia thereof) re-  
3       ceiving such grants may partner with one or more  
4       government laboratories or for-profit institutions.

5           (2) MERIT REVIEW; COMPETITION.—Grants  
6       shall be awarded under this subsection on a merit-  
7       reviewed competitive basis.

8           (3) PURPOSE.—The purpose of the Centers  
9       shall be to generate innovative approaches to com-  
10      puter and network security by conducting cutting-  
11      edge, multidisciplinary research in computer and  
12      network security, including the research areas de-  
13      scribed in subsection (a)(1).

14          (4) APPLICATIONS.—An institution of higher  
15      education (or a consortium of such institutions)  
16      seeking funding under this subsection shall submit  
17      an application to the Director at such time, in such  
18      manner, and containing such information as the Di-  
19      rector may require. The application shall include, at  
20      a minimum, a description of—

21           (A) the research projects that will be un-  
22           dertaken by the Center and the contributions of  
23           each of the participating entities;

24           (B) how the Center will promote active col-  
25           laboration among scientists and engineers from

1 different disciplines, such as computer sci-  
2 entists, engineers, mathematicians, and social  
3 science researchers;

4 (C) how the Center will contribute to in-  
5 creasing the number of computer and network  
6 security researchers and other professionals  
7 among all cultures; and

8 (D) how the center will disseminate re-  
9 search results quickly and widely to improve  
10 cybersecurity in information technology net-  
11 works, products, and services.

12 (5) CRITERIA.—In evaluating the applications  
13 submitted under paragraph (4), the Director shall  
14 consider, at a minimum—

15 (A) the ability of the applicant to generate  
16 innovative approaches to computer and network  
17 security and effectively carry out the research  
18 program;

19 (B) the experience of the applicant in con-  
20 ducting research on computer and network se-  
21 curity and the capacity of the applicant to fos-  
22 ter new multidisciplinary collaborations;

23 (C) the capacity of the applicant to attract  
24 and provide adequate support for a diverse  
25 group of undergraduate and graduate students

1 and postdoctoral fellows to pursue computer  
2 and network security research; and

3 (D) the extent to which the applicant will  
4 partner with government laboratories or for-  
5 profit entities, and the role the government lab-  
6 oratories or for-profit entities will play in the  
7 research undertaken by the Center.

8 (6) ANNUAL MEETING.—The Director shall  
9 convene an annual meeting of the Centers in order  
10 to foster collaboration and communication between  
11 Center participants.

12 (7) AUTHORIZATION OF APPROPRIATIONS.—  
13 There are authorized to be appropriated for the Na-  
14 tional Science Foundation to carry out this  
15 subsection—

16 (A) \$12,000,000 for fiscal year 2003;  
17 (B) \$24,000,000 for fiscal year 2004;  
18 (C) \$36,000,000 for fiscal year 2005;  
19 (D) \$36,000,000 for fiscal year 2006; and  
20 (E) \$36,000,000 for fiscal year 2007.

21 **SEC. 5. NATIONAL SCIENCE FOUNDATION COMPUTER AND**  
22 **NETWORK SECURITY PROGRAMS.**

23 (a) COMPUTER AND NETWORK SECURITY CAPACITY  
24 BUILDING GRANTS.—



1           (1) IN GENERAL.—The Director shall establish  
2           a program to award grants to institutions of higher  
3           education (or consortia thereof) to establish or im-  
4           prove undergraduate and master’s degree programs  
5           in computer and network security, to increase the  
6           number and diversity of students who pursue under-  
7           graduate or master’s degrees in fields related to  
8           computer and network security, and to provide stu-  
9           dents with experience in government or industry re-  
10          lated to their computer and network security studies.

11          (2) MERIT REVIEW.—Grants shall be awarded  
12          under this subsection on a merit-reviewed competi-  
13          tive basis.

14          (3) USE OF FUNDS.—Grants awarded under  
15          this subsection shall be used for activities that en-  
16          hance the ability of an institution of higher edu-  
17          cation (or consortium thereof) to provide high-qual-  
18          ity undergraduate and master’s degree programs in  
19          computer and network security and to recruit and  
20          retain increased numbers of students to such pro-  
21          grams. Activities may include—

22                (A) revising curriculum to better prepare  
23                undergraduate and master’s degree students for  
24                careers in computer and network security;

1 (B) establishing degree and certificate pro-  
2 grams in computer and network security;

3 (C) creating opportunities for under-  
4 graduate students to participate in computer  
5 and network security research projects;

6 (D) acquiring equipment necessary for stu-  
7 dent instruction in computer and network secu-  
8 rity, including the installation of testbed net-  
9 works for student use;

10 (E) providing opportunities for faculty to  
11 work with local or Federal Government agen-  
12 cies, private industry, or other academic institu-  
13 tions to develop new expertise or to formulate  
14 new research directions in computer and net-  
15 work security;

16 (F) establishing collaborations with other  
17 academic institutions or departments that seek  
18 to establish, expand, or enhance programs in  
19 computer and network security;

20 (G) establishing student internships in  
21 computer and network security at government  
22 agencies or in private industry;

23 (H) establishing collaborations with other  
24 academic institutions to establish or enhance a  
25 web- based collection of computer and network

1 security courseware and laboratory exercises for  
2 sharing with other institutions of higher edu-  
3 cation and community colleges;

4 (I) providing outreach to teachers in kin-  
5 dergarten through grade 12 to increase their  
6 awareness, and the awareness of their students,  
7 of computer security careers and practices; and

8 (J) establishing or enhancing bridge pro-  
9 grams in computer and network security be-  
10 tween community colleges and universities; and

11 (K) any other activities the Director deter-  
12 mines will accomplish the goals of this sub-  
13 section.

14 (4) SELECTION PROCESS.—

15 (A) APPLICATION.—An institution of high-  
16 er education (or a consortium thereof) seeking  
17 funding under this subsection shall submit an  
18 application to the Director at such time, in such  
19 manner, and containing such information as the  
20 Director may require. The application shall in-  
21 clude, at a minimum—

22 (i) a description of the applicant's  
23 computer and network security research  
24 and instructional capacity, and in the case  
25 of an application from a consortium of in-

1                   stitutions of higher education, a descrip-  
2                   tion of the role that each member will play  
3                   in implementing the proposal;

4                   (ii) a comprehensive plan by which the  
5                   institution or consortium will build instruc-  
6                   tional capacity in computer and informa-  
7                   tion security;

8                   (iii) a description of relevant collabo-  
9                   rations with government agencies or pri-  
10                  vate industry that inform the instructional  
11                  program in computer and network secu-  
12                  rity;

13                  (iv) a survey of the applicant's his-  
14                  toric student enrollment and placement  
15                  data in fields related to computer and net-  
16                  work security and a study of potential en-  
17                  rollment and placement for students en-  
18                  rolled in the proposed computer and net-  
19                  work security program; and

20                  (v) a plan to evaluate the success of  
21                  the proposed computer and network secu-  
22                  rity program, including post-graduation as-  
23                  sessment of graduate school and job place-  
24                  ment and retention rates as well as the rel-

1 evance of the instructional program to  
2 graduate study and to the workplace.

3 (B) AWARDS.—(i) The Director shall en-  
4 sure, to the extent practicable, that grants are  
5 awarded under this subsection in a wide range  
6 of geographic areas and categories of institu-  
7 tions of higher education, including minority  
8 serving institutions.

9 (ii) The Director shall award grants under  
10 this subsection for a period not to exceed 5  
11 years.

12 (5) ASSESSMENT REQUIRED.—The Director  
13 shall evaluate the program established under this  
14 subsection no later than 6 years after the establish-  
15 ment of the program. At a minimum, the Director  
16 shall evaluate the extent to which the grants  
17 achieved their objectives of increasing the quality,  
18 quantity, and diversity of students pursuing under-  
19 graduate or master's degrees in computer and net-  
20 work security.

21 (6) AUTHORIZATION OF APPROPRIATIONS.—  
22 There are authorized to be appropriated to the Na-  
23 tional Science Foundation to carry out this  
24 subsection—

25 (A) \$15,000,000 for fiscal year 2003;

- 1 (B) \$20,000,000 for fiscal year 2004;  
2 (C) \$20,000,000 for fiscal year 2005;  
3 (D) \$20,000,000 for fiscal year 2006; and  
4 (E) \$20,000,000 for fiscal year 2007.

5 (b) SCIENTIFIC AND ADVANCED TECHNOLOGY ACT  
6 OF 1992.—

7 (1) GRANTS.—The Director shall provide  
8 grants under the Scientific and Advanced Tech-  
9 nology Act of 1992 (42 U.S.C. 1862i) for the pur-  
10 poses of section 3(a) and (b) of that Act, except that  
11 the activities supported pursuant to this subsection  
12 shall be limited to improving education in fields re-  
13 lated to computer and network security.

14 (2) AUTHORIZATION OF APPROPRIATIONS.—  
15 There are authorized to be appropriated to the Na-  
16 tional Science Foundation to carry out this  
17 subsection—

- 18 (A) \$1,000,000 for fiscal year 2003;  
19 (B) \$1,250,000 for fiscal year 2004;  
20 (C) \$1,250,000 for fiscal year 2005;  
21 (D) \$1,250,000 for fiscal year 2006; and  
22 (E) \$1,250,000 for fiscal year 2007.

23 (c) GRADUATE TRAINEESHIPS IN COMPUTER AND  
24 NETWORK SECURITY RESEARCH.—

1           (1) IN GENERAL.—The Director shall establish  
2           a program to award grants to institutions of higher  
3           education to establish traineeship programs for  
4           graduate students who pursue computer and net-  
5           work security research leading to a doctorate degree  
6           by providing funding and other assistance, and by  
7           providing graduate students with research experience  
8           in government or industry related to the students'  
9           computer and network security studies.

10          (2) MERIT REVIEW.—Grants shall be provided  
11          under this subsection on a merit-reviewed competi-  
12          tive basis.

13          (3) USE OF FUNDS.—An institution of higher  
14          education shall use grant funds for the purposes  
15          of—

16                (A) providing fellowships to students who  
17                are citizens, nationals, or lawfully admitted per-  
18                manent resident aliens of the United States and  
19                are pursuing research in computer or network  
20                security leading to a doctorate degree;

21                (B) paying tuition and fees for students  
22                receiving fellowships under subparagraph (A);

23                (C) establishing scientific internship pro-  
24                grams for students receiving fellowships under  
25                subparagraph (A) in computer and network se-

1           curity at for-profit institutions or government  
2           laboratories; and

3           (D) other costs associated with the admin-  
4           istration of the program.

5           (4) FELLOWSHIP AMOUNT.—Fellowships pro-  
6           vided under paragraph (3)(A) shall be in the amount  
7           of \$25,000 per year, or the level of the National  
8           Science Foundation Graduate Research Fellowships,  
9           whichever is greater, for up to 3 years.

10          (5) SELECTION PROCESS.—An institution of  
11          higher education seeking funding under this sub-  
12          section shall submit an application to the Director at  
13          such time, in such manner, and containing such in-  
14          formation as the Director may require. The applica-  
15          tion shall include, at a minimum, a description of—

16                (A) the instructional program and research  
17                opportunities in computer and network security  
18                available to graduate students at the applicant's  
19                institution; and

20                (B) the internship program to be estab-  
21                lished, including the opportunities that will be  
22                made available to students for internships at  
23                for-profit institutions and government labora-  
24                tories.



1           (6) REVIEW OF APPLICATIONS.—In evaluating  
2           the applications submitted under paragraph (5), the  
3           Director shall consider—

4                   (A) the ability of the applicant to effec-  
5                   tively carry out the proposed program;

6                   (B) the quality of the applicant's existing  
7                   research and education programs;

8                   (C) the likelihood that the program will re-  
9                   cruit increased numbers and a more diverse  
10                  population of students to pursue and earn doc-  
11                  torate degrees in computer and network secu-  
12                  rity;

13                  (D) the nature and quality of the intern-  
14                  ship program established through collaborations  
15                  with government laboratories and for-profit in-  
16                  stitutions;

17                  (E) the integration of internship opportu-  
18                  nities into graduate students' research; and

19                  (F) the relevance of the proposed program  
20                  to current and future computer and network se-  
21                  curity needs.

22           (7) AUTHORIZATION OF APPROPRIATIONS.—  
23           There are authorized to be appropriated to the Na-  
24           tional Science Foundation to carry out this  
25           subsection—

- 1 (A) \$10,000,000 for fiscal year 2003;
- 2 (B) \$20,000,000 for fiscal year 2004;
- 3 (C) \$20,000,000 for fiscal year 2005;
- 4 (D) \$20,000,000 for fiscal year 2006; and
- 5 (E) \$20,000,000 for fiscal year 2007.

6 (d) GRADUATE RESEARCH FELLOWSHIPS PROGRAM  
7 SUPPORT.—Computer and network security shall be in-  
8 cluded among the fields of specialization supported by the  
9 National Science Foundation’s Graduate Research Fellow-  
10 ships program under section 10 of the National Science  
11 Foundation Act of 1950 (42 U.S.C. 1869).

12 (e) CYBERSECURITY FACULTY DEVELOPMENT FEL-  
13 LOWSHIP PROGRAM.—

14 (1) IN GENERAL.—The Director shall establish  
15 a program to award grants to institutions of higher  
16 education to establish traineeship programs to en-  
17 able graduate students to pursue academic careers  
18 in cybersecurity upon completion of doctoral degrees.

19 (2) APPLICATION.—Each institution of higher  
20 education desiring to receive a grant under this sub-  
21 section shall submit an application to the Director at  
22 such time, in such manner, and containing such in-  
23 formation as the Director shall require.

1           (3) USE OF FUNDS.—Funds received by an in-  
2           stitution of higher education under this paragraph  
3           shall—

4                   (A) be made available to individuals on a  
5                   merit-reviewed competitive basis and in accord-  
6                   ance with the procedures established in para-  
7                   graph (5);

8                   (B) be in an amount that is sufficient to  
9                   cover annual tuition and fees for doctoral study  
10                  at an institution of higher education for the du-  
11                  ration of the graduate fellowship, and shall in-  
12                  clude, in addition, an annual living stipend of  
13                  \$25,000; and

14                  (C) be provided to individuals for a dura-  
15                  tion of no more than 3 to 5 years, the specific  
16                  duration of each graduate fellowship to be de-  
17                  termined by the institution of higher education,  
18                  on a case-by- case basis.

19           (4) REPAYMENT.—Each graduate fellowship  
20           shall—

21                   (A) subject to subparagraph (4)(B), be  
22                   subject to full repayment upon completion of  
23                   the doctoral degree according to a repayment  
24                   schedule established and administered by the  
25                   institution of higher education;

1 (B) be forgiven at the rate of 20 percent  
2 of the total amount of the graduate fellowship  
3 assistance received under this section for each  
4 academic year that a recipient is employed as a  
5 full-time faculty member at an institution of  
6 higher education for a period not to exceed 5  
7 years; and

8 (C) be monitored by the institution of  
9 higher education to ensure compliance with this  
10 subsection.

11 (5) ELIGIBILITY.—To be eligible to receive a  
12 graduate fellowship under this section, an individual  
13 shall—

14 (A) be a citizen, national, or lawfully ad-  
15 mitted permanent resident alien of the United  
16 States;

17 (B) demonstrate a commitment to a career  
18 in higher education.

19 (6) CONSIDERATION.—In making selections for  
20 graduate fellowships under this paragraph, the Di-  
21 rector, to the extent possible and in consultation  
22 with institutions of higher education, shall consider  
23 a diverse pool of applicants whose interests are of an  
24 interdisciplinary nature, encompassing the social sci-

1       entific as well as the technical dimensions of  
2       cybersecurity.

3               (7) AUTHORIZATION OF APPROPRIATIONS.—

4       There are authorized to be appropriated to the Na-  
5       tional Science Foundation to carry out this para-  
6       graph \$5,000,000 for each of fiscal years 2003  
7       through 2007.

8       **SEC. 6. CONSULTATION.**

9       In carrying out sections 4 and 5, the Director shall  
10      consult with other Federal agencies.

11      **SEC. 7. FOSTERING RESEARCH AND EDUCATION IN COM-**

12                      **PUTER AND NETWORK SECURITY.**

13      Section 3(a) of the National Science Foundation Act  
14      of 1950 (42 U.S.C. 1862(a)) is amended—

15              (1) by striking “and” at the end of paragraph  
16      (6);

17              (2) by striking “Congress.” in paragraph (7)  
18      and inserting “Congress ; and”; and

19              (3) by adding at the end the following:

20              “(8) to take a leading role in fostering and sup-  
21      porting research and education activities to improve  
22      the security of networked information systems.”.

1 **SEC. 8. NATIONAL INSTITUTE OF STANDARDS AND TECH-**  
2 **NOLOGY PROGRAMS.**

3 (a) RESEARCH PROGRAM.—The National Institute of  
4 Standards and Technology Act is amended—

5 (1) by moving section 22 to the end of the Act  
6 and redesignating it as section 32;

7 (2) by inserting after section 21 the following  
8 new section:

9 “RESEARCH PROGRAM ON SECURITY OF COMPUTER  
10 SYSTEMS

11 “SEC. 22. (a) ESTABLISHMENT.—The Director,  
12 through the Director of the Office for Information Secu-  
13 rity Programs, shall establish a program of assistance to  
14 institutions of higher education that enter into partner-  
15 ships with for-profit entities to support research to im-  
16 prove the security of computer systems. The partnerships  
17 may also include government laboratories. The program  
18 shall—

19 “(1) include multidisciplinary, long-term re-  
20 search;

21 “(2) include research directed toward address-  
22 ing needs identified through the activities of the  
23 Computer System Security and Privacy Advisory  
24 Board under section 20(f); and

25 “(3) promote the development of a robust re-  
26 search community working at the leading edge of

1 knowledge in subject areas relevant to the security  
2 of computer systems by providing support for grad-  
3 uate students, post-doctoral researchers, and senior  
4 researchers.

5 “(b) FELLOWSHIPS.—

6 “(1) IN GENERAL.—The Director is authorized  
7 to establish a program to award post-doctoral re-  
8 search fellowships to individuals who are citizens,  
9 nationals, or lawfully admitted permanent resident  
10 aliens of the United States and are seeking research  
11 positions at institutions, including the Institute, en-  
12 gaged in research activities related to the security of  
13 computer systems, including the research areas de-  
14 scribed in section 4(a)(1) of the Cyber Security Re-  
15 search and Development Act.

16 “(2) SENIOR RESEARCH FELLOWSHIPS.—The Direc-  
17 tor is authorized to establish a program to award senior  
18 research fellowships to individuals seeking research posi-  
19 tions at institutions, including the Institute, engaged in  
20 research activities related to the security of computer sys-  
21 tems, including the research areas described in section  
22 4(a)(1) of the Cyber Security Research and Development  
23 Act. Senior research fellowships shall be made available  
24 for established researchers at institutions of higher edu-

1 cation who seek to change research fields and pursue stud-  
2 ies related to the security of computer systems.

3 “(3) Eligibility.—

4 “(A) IN GENERAL.—To be eligible for an  
5 award under this subsection, an individual shall  
6 submit an application to the Director at such  
7 time, in such manner, and containing such in-  
8 formation as the Director may require.

9 “(B) STIPENDS.—Under this subsection, the Direc-  
10 tor is authorized to provide stipends for post-doctoral re-  
11 search fellowships at the level of the Institute’s Post Doc-  
12 toral Research Fellowship Program and senior research  
13 fellowships at levels consistent with support for a faculty  
14 member in a sabbatical position.

15 “(c) AWARDS; APPLICATIONS.—

16 “(1) IN GENERAL.—The Director is authorized  
17 to award grants or cooperative agreements to insti-  
18 tutions of higher education to carry out the program  
19 established under subsection (a).

20 “(2) ELIGIBILITY.—To be eligible for an award  
21 under this section, an institution of higher education  
22 shall submit an application to the Director at such  
23 time, in such manner, and containing such informa-  
24 tion as the Director may require. The application  
25 shall include, at a minimum, a description of—



1           “(A) the number of graduate students an-  
2           ticipated to participate in the research project  
3           and the level of support to be provided to each;

4           “(B) the number of post-doctoral research  
5           positions included under the research project  
6           and the level of support to be provided to each;

7           “(C) the number of individuals, if any, in-  
8           tending to change research fields and pursue  
9           studies related to the security of computer sys-  
10          tems to be included under the research project  
11          and the level of support to be provided to each;  
12          and

13          “(D) how the for-profit entities and any  
14          other partners will participate in developing and  
15          carrying out the research and education agenda  
16          of the partnership.

17          “(d) SLIDING SCALE COST-SHARING.—In awarding a  
18          grant under this section, the Director shall require up to  
19          50 percent of the costs of the project funded by the grant  
20          to be met by the for-profit entity or entities in the partner-  
21          ship. The Director shall base the percentage of cost-shar-  
22          ing required under this paragraph on a sliding scale re-  
23          flecting the degree to which the results of the research  
24          undertaken by a partnership may reasonably be expected  
25          to be applied and shared, with—

1           “(1) the smallest percentage of cost-sharing re-  
2           quired for projects the anticipated results of which  
3           are reasonably expected to be of broadest potential  
4           application and broadly shared; and

5           “(2) the greatest percentage of cost-sharing re-  
6           quired for projects the anticipated results of which  
7           are reasonably expected—

8           “(A) to be of narrow or proprietary appli-  
9           cation; or

10           “(B) not to be broadly shared.

11           “(e) PROGRAM OPERATION.—

12           “(1) MANAGEMENT.—The program established  
13           under subsection (a) shall be headed by the Director  
14           of the Office for Information Security Programs and  
15           managed by individuals who shall have both exper-  
16           tise in research related to the security of computer  
17           systems and knowledge of the vulnerabilities of exist-  
18           ing computer systems. The Director shall designate  
19           such individuals, on a competitive basis, as program  
20           managers.

21           “(2) MANAGERS MAY BE EMPLOYEES.—Program  
22           managers designated under paragraph (1) may be new or  
23           existing employees of the Institute.

1       “(3) MANAGER RESPONSIBILITY.—Program man-  
2 agers designated under paragraph (1) shall be responsible  
3 for—

4           “(A) establishing and publicizing the broad re-  
5 search goals for the program;

6           “(B) soliciting applications for specific research  
7 projects to address the goals developed under sub-  
8 paragraph (A);

9           “(C) selecting research projects for support  
10 under the program from among applications sub-  
11 mitted to the Institute, following consideration of—

12           “(i) the novelty and scientific and technical  
13 merit of the proposed projects;

14           “(ii) the demonstrated capabilities of the  
15 individual or individuals submitting the applica-  
16 tions to successfully carry out the proposed re-  
17 search;

18           “(iii) the impact the proposed projects will  
19 have on increasing the number of computer se-  
20 curity researchers;

21           “(iv) the nature of the participation by for-  
22 profit entities and the extent to which the pro-  
23 posed projects address the concerns of industry;  
24 and

1                   “(v) other criteria determined by the Di-  
2                   rector, based on information specified for inclu-  
3                   sion in applications under subsection (c); and

4                   “(D) monitoring the progress of research  
5                   projects supported under the program.

6                   “(4) From amounts available for awards under sub-  
7                   section (c), the Director, in consultation with the Director  
8                   of the Office for Information Security Programs estab-  
9                   lished in section 20 of this Act, may assign up to 5 percent  
10                  to a Directors Fund which may be awarded throughout  
11                  the fiscal year at the discretion of the Director to prom-  
12                  ising projects designed to fulfill the goals stated in sub-  
13                  section (a). Such projects should be innovative in nature  
14                  and should meet emerging needs in computer security.

15                  “(f) REVIEW OF PROGRAM.—

16                  “(1) PERIODIC REVIEW.—The Director shall  
17                  periodically review the portfolio of research awards  
18                  monitored by each program manager designated in  
19                  accordance with subsection (e). In conducting those  
20                  reviews, the Director shall seek the advice of the  
21                  Computer System Security and Privacy Advisory  
22                  Board, established under section 21, on the appro-  
23                  priateness of the research goals and on the quality  
24                  and utility of research projects managed by program  
25                  managers in accordance with subsection (e).

1       “(2) COMPREHENSIVE 5-YEAR REVIEW.—The Direc-  
2       tor shall also contract with the National Research Council  
3       for a comprehensive review of the program established  
4       under subsection (a) during the 5th year of the program.  
5       Such review shall include an assessment of the scientific  
6       quality of the research conducted, the relevance of the re-  
7       search results obtained to the goals of the program estab-  
8       lished under subsection (e)(3)(A), and the progress of the  
9       program in promoting the development of a substantial  
10      academic research community working at the leading edge  
11      of knowledge in the field. The Director shall submit to  
12      Congress a report on the results of the review under this  
13      paragraph no later than 6 years after the initiation of the  
14      program.

15      “(g) DEFINITIONS.—In this section:

16           “(1) COMPUTER SYSTEM.—The term ‘computer  
17           system’ has the meaning given that term in section  
18           20(d)(1).

19           “(2) INSTITUTION OF HIGHER EDUCATION.—  
20           The term ‘institution of higher education’ has the  
21           meaning given that term in section 101 of the High-  
22           er Education Act of 1965 (20 U.S.C. 1001).’.”.

23           (b) AMENDMENT OF COMPUTER SYSTEM DEFINI-  
24           TION.—Section 20(d)(1)(B)(i) of National Institute of

1 Standards and Technology Act (15 U.S.C. 278g-  
2 3(d)(1)(B)(i)) is amended to read as follows:

3 “(i) computers and computer net-  
4 works;”.

5 (c) APPROPRIATE FEDERAL AGENCY BENCHMARK  
6 SECURITY STANDARDS.—

7 (1) NIST REPORT.—Not later than 180 days  
8 after the date of enactment of this Act, the Director  
9 of the National Institute of Standards and Tech-  
10 nology shall submit to Committee on Commerce,  
11 Science, and Transportation of the Senate, the Com-  
12 mittee on Science of the House of Representatives,  
13 and the Committees on Appropriations of the Senate  
14 and the House of Representatives a report that—

15 (A) identifies specific Federal agency  
16 benchmark security standards that should be  
17 developed by the Institute over the 12-month  
18 period beginning on the date of the report, and  
19 that should serve as the basis for security  
20 standards that will eventually be adopted by the  
21 departments and agencies of the Federal Gov-  
22 ernment; and

23 (B) recommends, in consultation with the  
24 Office of Management and Budget, any Federal  
25 funding, in addition to levels authorized under

1           this title, that the Institute requires fully to  
2           carry out its mission under this title.

3           (2) NIST RECOMMENDATIONS FOR FEDERAL  
4           AGENCY BENCHMARK STANDARDS.—

5                   (A) IN GENERAL.—Not later than 1 year  
6           after the date of the report issued under para-  
7           graph (1), Director of the National Institute of  
8           Standards and Technology shall, in consultation  
9           with appropriate public and private entities,  
10          prepare a report for the Secretary of Commerce  
11          and the Chairman of the Federal Chief Infor-  
12          mation Officers council that contains rec-  
13          ommendations for specific, reasonable Federal  
14          agency benchmark security standards to be  
15          adopted by the civilian departments and agen-  
16          cies of the Federal Government.

17                   (B) UPDATES.—The Director shall review  
18          the recommended standards under subpara-  
19          graph (A) not less than once every 6 months,  
20          and update such standards or issue new stand-  
21          ards as necessary. Nothing in this title shall  
22          prohibit the Director from updating any portion  
23          of such recommended standards more fre-  
24          quently if determines that circumstances so re-  
25          quire.

1 (C) DISSEMINATION.—The Secretary of  
2 Commerce shall widely disseminate the report  
3 under subparagraph (A), and any update of the  
4 report under subparagraph (B), among relevant  
5 government (including State and local govern-  
6 ment), private and academic entities.

7 (3) ADOPTION OF BENCHMARK SECURITY  
8 STANDARDS GOVERNMENT-WIDE.—

9 (A) IN GENERAL.—Not later than 90 days  
10 after the date of the report under paragraph  
11 (2)(A), each civilian department and agency of  
12 the Federal Government shall implement the  
13 appropriate benchmark security standards rec-  
14 ommended by such report.

15 (B) IMPLEMENTATION OF UPDATED  
16 STANDARDS.—If the Director of the National  
17 Institute of Standards and Technology, through  
18 the Secretary of Commerce, updates rec-  
19 ommended federal agency benchmark security  
20 standards pursuant to paragraph (2), each civil-  
21 ian department and agency of the Federal Gov-  
22 ernment shall implement such updated stand-  
23 ards not later than 30 days after the date of  
24 the report containing recommendations for up-  
25 dated standards.



1 (C) IMPLEMENTATION OF NEW STAND-  
2 ARDS.—If the Director of the National Institute  
3 of Standards and Technology, through the Sec-  
4 retary of Commerce, recommends new Federal  
5 agency benchmark security standards pursuant  
6 to paragraph (2), each civilian department and  
7 agency of the Federal Government shall imple-  
8 ment such new standards no later than 90 days  
9 after the date of the report containing rec-  
10 ommendations for new standards.

11 (4) CURRENT FEDERAL AGENCY BENCHMARK  
12 SECURITY STANDARDS.—

13 (A) IN GENERAL.—Not later than 90 days  
14 after the date of enactment of this Act, the Di-  
15 rector of the Chairman of the Federal Chief In-  
16 formation Officers Council shall provide to the  
17 Director of the National Institute of Standards  
18 and Technology a list of the specific bench-  
19 marks that each civilian department and agency  
20 of the Federal Government uses as its current  
21 minimum security standards.

22 (B) CLASSIFIED REPORT.—The list under  
23 this paragraph shall be provided in classified  
24 form.

1           (5) AUTHORIZATION OF APPROPRIATIONS.—

2       There are hereby authorized to be appropriated for  
3       the National Institute of Standards and Technology  
4       for purposes of activities under this Act,  
5       \$15,000,000 for each of fiscal years 2003 through  
6       2007

7       (d) REPORTS TO CONGRESS.—

8           (1) FEDERAL CHIEF INFORMATION OFFICERS  
9       REPORT.—Not later than 36 months after the date  
10      of enactment of this Act, the Chairman of Federal  
11      Chief Information Officers Council shall submit a re-  
12      port to the appropriate committees of Congress  
13      including—

14           (A) a description of the status of imple-  
15           mentation of the federal agency benchmark se-  
16           curity standards at each department and agen-  
17           cy of the Federal Government;

18           (B) a description of the costs associated  
19           with such implementation; and

20           (C) a description of any barriers to imple-  
21           mentation and recommendation for overcoming  
22           such barriers.

23           (2) NATIONAL ACADEMY OF SCIENCES  
24       STUDY.—Not later than 3 months after the date of  
25       enactment of this Act, the Director of the National

1 Institute of Standards and Technology shall enter  
2 into an arrangement with the National Research  
3 Council of the National Academy of Sciences to con-  
4 duct a study to examine the impact of requiring  
5 Federal agencies to implement benchmark security  
6 standards on the state of national cybersecurity pre-  
7 paredness.

8 (A) MATTERS TO BE ASSESSED IN  
9 STUDY.—At a minimum, the study shall ad-  
10 dress the following:

11 (i) The extent to which the  
12 cybersecurity posture of federal agencies  
13 would be improved with the adoption of the  
14 standards described in subsection  
15 (c)(2)(A).

16 (ii) The operational benefits, costs  
17 and consequences of the adoption of the  
18 standards described in subsection  
19 (c)(2)(A).

20 (iii) The operational consequences of  
21 differing cybersecurity needs for different  
22 Federal agencies.

23 (B) CLASSIFIED REPORT.—To the max-  
24 imum degree possible, the final report shall be

1 submitted in unclassified form with classified  
2 annexes as necessary.

3 (C) INTERAGENCY COOPERATION WITH  
4 STUDY.—All Federal agencies shall cooperate  
5 fully with the National Research Council in its  
6 activities in carrying out the study under this  
7 section.

8 (D) EXPEDITED PROCESSING OF SECURITY  
9 CLEARANCES FOR STUDY.—For the purpose of  
10 facilitating the commencement of the study  
11 under this section, officials in relevant depart-  
12 ments and agencies of the Federal Government  
13 shall expedite to the fullest degree possible the  
14 processing of security clearances that are nec-  
15 essary for the National Research Council to  
16 conduct the study.

17 (E) REPORT.—The Director of the Na-  
18 tional Institute of Standards and Technology  
19 shall transmit a report to containing the results  
20 of the study to the Congress not later than 21  
21 months after the date of enactment of this Act.

22 (F) AUTHORIZATION OF APPROPRIA-  
23 TIONS.—There are authorized to be appro-  
24 priated to the Secretary of Commerce for the  
25 National Institute of Standards and Technology

1           for the purposes of carrying out this subsection,  
2           \$800,000.

3           (e) INFORMATION SECURITY PROGRAM OFFICE.—  
4 Section 20 of the National Institute of Standards and  
5 Technology Act (15 U.S.C. 278g-3), is amended by redes-  
6 ignating subsection (d) as subsection (e) and by inserting  
7 after subsection (c) the following:

8           “(d) ESTABLISHMENT OF AN OFFICE FOR INFORMA-  
9 TION SECURITY PROGRAMS.—

10                   “(1) IN GENERAL.—There is established in  
11 the Institute an Office for Information Security  
12 Programs.

13                   “(2) HEAD.—The Office for Information  
14 Security Programs shall be headed by a Direc-  
15 tor, who shall be a senior executive and shall be  
16 compensated at a level in the Senior Executive  
17 Service under section 5382 of title 5, United  
18 States Code, as determined by the Secretary of  
19 Commerce.

20                   “(3) FUNCTION.—The Director of the In-  
21 stitute shall delegate to the Director of the Of-  
22 fice of Information Security Programs the au-  
23 thority to administer all functions under this  
24 section, except that any such delegation shall  
25 not relieve the Director of the Institute of re-

1           sponsibility for the administration of such func-  
2           tions. The Director of the Office of Information  
3           Security Programs shall serve as principal ad-  
4           viser to the Director of the Institute on all  
5           functions under this section.”

6   **SEC. 9. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS,**  
7                           **AND INFORMATION.**

8           Section 20 of the National Institute of Standards and  
9   Technology Act (15 U.S.C. 278g–3) is amended by adding  
10   at the end the following new subsection:

11          “(f) AUTHORIZATION OF APPROPRIATIONS.—There  
12   are authorized to be appropriated to the Secretary  
13   \$1,060,000 for fiscal year 2003 and \$1,090,000 for fiscal  
14   year 2004 to enable the Computer System Security and  
15   Privacy Advisory Board, established by section 21, to iden-  
16   tify emerging issues, including research needs, related to  
17   computer security, privacy, and cryptography and, as ap-  
18   propriate, to convene public meetings on those subjects,  
19   receive presentations, and publish reports, digests, and  
20   summaries for public distribution on those subjects.”.

21   **SEC. 10. INTRAMUTAL SECURITY RESEARCH.**

22          Section 20 of the National Institute of Standards and  
23   Technology Act (15 U.S.C. 278g–3), as amended by this  
24   Act, is further amended by redesignating subsection (f)

1 as subsection (g), and by inserting after subsection (e) the  
2 following:

3 “(g) INTRAMURAL SECURITY RESEARCH.—As part of  
4 the research activities conducted in accordance with sub-  
5 section (b)(4), the Institute shall—

6 “(1) conduct a research program to address  
7 emerging technologies associated with assembling a  
8 networked computer system from components while  
9 ensuring it maintains desired security properties;

10 “(2) carry out research associated with improv-  
11 ing the security of real-time computing and commu-  
12 nications systems for use in process control; and

13 “(3) carry out multidisciplinary, long-term,  
14 high-risk research on ways to improve the security  
15 of computer systems.”.

16 **SEC. 11. AUTHORIZATION OF APPROPRIATIONS.**

17 There are authorized to be appropriated to the Sec-  
18 retary of Commerce for the National Institute of Stand-  
19 ards and Technology—

20 (1) for activities under section 22 of the Na-  
21 tional Institute of Standards and Technology Act, as  
22 added by section 8 of this Act—

23 (A) \$25,000,000 for fiscal year 2003;

24 (B) \$40,000,000 for fiscal year 2004;

25 (C) \$55,000,000 for fiscal year 2005;

1 (D) \$70,000,000 for fiscal year 2006;

2 (E) \$85,000,000 for fiscal year 2007; and

3 (2) for activities under section 20(f) of the Na-  
4 tional Institute of Standards and Technology Act, as  
5 added by section 10 of this Act—

6 (A) \$6,000,000 for fiscal year 2003;

7 (B) \$6,200,000 for fiscal year 2004;

8 (C) \$6,400,000 for fiscal year 2005;

9 (D) \$6,600,000 for fiscal year 2006; and

10 (E) \$6,800,000 for fiscal year 2007.

11 **SEC. 12. NATIONAL ACADEMY OF SCIENCES STUDY ON**  
12 **COMPUTER AND NETWORK SECURITY IN**  
13 **CRITICAL INFRASTRUCTURES.**

14 (a) STUDY.—Not later than 3 months after the date  
15 of the enactment of this Act, the Director of the National  
16 Institute of Standards and Technology shall enter into an  
17 arrangement with the National Research Council of the  
18 National Academy of Sciences to conduct a study of the  
19 vulnerabilities of the Nation’s network infrastructure and  
20 make recommendations for appropriate improvements.  
21 The National Research Council shall—

22 (1) review existing studies and associated data  
23 on the architectural, hardware, and software  
24 vulnerabilities and interdependencies in United  
25 States critical infrastructure networks;



1           (2) identify and assess gaps in technical capa-  
2           bility for robust critical infrastructure network secu-  
3           rity, and make recommendations for research prior-  
4           ities and resource requirements; and

5           (3) review any and all other essential elements  
6           of computer and network security, including security  
7           of industrial process controls, to be determined in  
8           the conduct of the study.

9           (b) REPORT.—The Director of the National Institute  
10          of Standards and Technology shall transmit a report con-  
11          taining the results of the study and recommendations re-  
12          quired by subsection (a) to the Congress not later than  
13          21 months after the date of enactment of this Act.

14          (c) SECURITY.—The Director of the National Insti-  
15          tute of Standards and Technology shall ensure that no in-  
16          formation that is classified is included in any publicly re-  
17          leased version of the report required by this section.

18          (d) AUTHORIZATION OF APPROPRIATIONS.—There  
19          are authorized to be appropriated to the Secretary of Com-  
20          merce for the National Institute of Standards and Tech-  
21          nology for the purposes of carrying out this section,  
22          \$700,000.

1   **SEC. 13. COORDINATION OF FEDERAL CYBER SECURITY RE-**  
2                   **SEARCH AND DEVELOPMENT**

3           Section 205 (a) of the National Science and Tech-  
4 nology Policy Act (42 U.S.C. 6614 (a)) is amended

5           (1) by striking “and” after the semicolon in  
6 paragraph (12);

7           (2) by redesignating paragraph (13) as para-  
8 graph (14); and

9           (3) by inserting after paragraph (12) the fol-  
10 lowing:

11           “(13) develop strategies, in consultation with  
12 the Office of Homeland Security, the President’s  
13 Critical Infrastructure Protection Board, and the  
14 relevant federal departments and agencies, to foster  
15 greater coordination of federal research and develop-  
16 ment activities and promote cooperation between the  
17 Federal Government, institutions of higher edu-  
18 cation, and private industry in the field of cyber se-  
19 curity; and”

○